REMARKS

Status of Claims

Claim 6 has been amended to address the examiner's objection. No other claim has been added, amended, or deleted. Claims 1-6 remain in the application.

Claim Objection – 37 CFR 1.75(c)

Claim 6 is objected to under 37 CFR 1.75(c) as allegedly being of improper dependent form. Applicant has revised claim 6 into proper dependent form. Withdrawal of the objection to claim 6 is solicited.

Claim Rejections – 35 USC §103(a)

Claims 1 and 5-6 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over US Pub. No. 2003/0097383 ("Smirnov") in view of USP 6,148,342 ("Ho"), USP 7,213,258 ("Kesarwani"), and US Pub. No. 2002/0174364 ("Nordman"). Also, claims 2-4 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Smirnov, Ho, Kesarwani, and Nordman in view of "what was well known in the art at the time of the invention." These rejections are respectfully traversed.

As noted in a previous response, the method of independent claim 1 permits the exchange of pseudonymous personal information between two or more data storage servers or within a data storage server in which the identities of persons, associated servers and/or associated organizations with which the personal information resides is pseudonymous. In accordance with the method, respective unique identifications (UIDs) are assigned to each person having private data for storage and each person is registered with a pseudonymous proxy server as at least one of a plurality of respective user types based on the respective person's relationship to the stored private data with associated pseudonyms for each user and sets of rules that control access to the respective person's stored private data and pseudonyms for the respective person's stored private data by persons registered with the pseudonymous proxy server based at least on user type. The persons are also provided with service provider identifiers that identify the respective persons to a service provider. The pseudonymous proxy server with which the person is registered provides each person's associated pseudonym and each person's service provider identifier with a random factor and enables

the transmission of a message from each person to the service provider. To accomplish the transmission, the pseudonymous proxy server receives the message and, based on the set of rules that control the person's access to the stored private data of a person registered with the pseudonymous proxy server, validates a relationship between the person and the service provider and transmits the message to the service provider if the relationship between the person and the service provider is validated. The pseudonymous proxy server also authorizes the person to view the stored private data of the person or pseudonyms for the private data of the person based on the set of rules that control the person's access to the stored private data of the person and the pseudonyms for the private data of the person.

In response to Applicant's previous arguments, the examiner now further alleges that Ho discloses registering user types and a service provider identifier and that Kesarwani discloses validating the person's relationship to the service provider so that access may be provided to private data. The examiner then essentially repeated the previous rejections. Applicant submits that the cited prior art does not suggest the combination of features of claim 1 and that the rejections of claims 1-6 should be withdrawn for at least the following additional reasons.

In rejecting claim 1, the examiner again alleges that Smirnov discloses registering the person with a pseudonymous proxy server as a user type with associated pseudonym, referencing paragraphs [0128] and [0132] of Smirnov. However, Smirnov simply teach the use of a "pseudonymity engine" so that neither the operator of the server nor the applications that query it are aware of the true identity of a data subject and without the users identifying themselves when they manipulate their records. Smirnov does not indicate that each person is assigned at least one of a plurality of *user types* based on the respective *person's relationship to the stored private data* as now claimed and does not teach controlling access to stored data based on a set of rules that limit access to the stored data by user type, for example. The examiner seems to suggest that the mere mention of a doctor selectively accessing a patient's data suggests that "user type" = "doctor" and suggests the relationship of that person to the stored data. Smirnov clearly does not relate the doctor to the stored data in this fashion. Instead, access is based on the doctor's relationship to the system on which the data is stored.

The examiner now alleges that Ho teaches "registering persons with a pseudonymous proxy server as at least one of a plurality of respective *user types* based on the respective person's relationship to the stored private data." In support, the examiner cites to column 3, lines 4-13, and column 4, lines 9-11, of Ho. In particular, the examiner alleges that the "type of user" is taught to be a doctor who is authorized to view the records of a particular patient. However, the examiner appears to have read too much into the teachings of Ho. Based on a careful review of the cited text, all that Ho teaches is that information is stored needed to identify an individual and that the subnetwork determines whether the user is a person authorized at a suitable access level to access the stored information for the individual. Contrary to the examiner's assertions, these passages in no way suggest that the user is registered with a pseudonymous proxy server based on the user's relationship to the stored private data of the individual, as opposed to the system on which the data is stored. In other words, the doctor is not registered to permit access as a service provider for the stored data of a particular patient. The cited passage says nothing of registering the doctor with a pseudonymous proxy server and nothing of registering the doctor based on his/her relationship to the stored data. Rather, the doctor's access is apparently based on a system access level of the doctor to the system on which the data is stored and generally says nothing of the doctor's relationship to the stored data. Thus, the doctor could be given access to the data of all patients without regard to the doctor's relationship to the patient or the patient's data. Accordingly, at least this feature is not taught by Ho.

The examiner now also alleges that Ho teaches a service provider identifier at column 3, lines 4-13, and that such information is accessed by a service provider such as a doctor, a lawyer, etc. as taught at column 2, lines 49-56. Applicant suggests that the examiner has misinterpreted the claimed feature. The examiner has apparently interpreted the stored private data as being the same as the service provider identifier in that the examiner alleges that the private data identifying the individual as taught by Ho at column 3, lines 4-13, is also a service provider identifier. This is not the case. The claimed service provider identifier identifies a person's pseudonym to a service provider while the data disclosed by Ho at column 3, lines 4-13, merely recites types of private data used to uniquely identify a person. Such data typically would not be a service provider identifier as that would defeat the purpose of keeping the private data confidential. This data is data that uniquely identifies a

patient to the system, for example, and does not register the patient's data with a particular service provider (*e.g.*, doctor). Nothing in Ho suggests otherwise. In any case, the examiner's interpretation of the claim language does not hold up under scrutiny.

In short, neither Smirnov nor Ho provides a "service provider identifier" that identifies the person's pseudonym to a service provider as claimed. An individual's stored private data (name, birth date, etc. at taught by Ho) is not used in the claimed method to identify the individual as that would defeat the purpose of pseudonymization. Though Ho notes at column 2, lines 49-56, that the person accessing private data may be a doctor, lawyer or other "service provider," neither Smirnov nor Ho provides any teachings that would have lead one skilled in the art to modify Smirnov to provide a relationship between a pseudonymous user and a service provider using a "service provider identifier" as claimed. Thus, even if Ho would have taught one skilled in the art to modify the Smirnov system to use IDs for the user and the subject, there is no teaching of further providing a "service provider identifier" as claimed. Moreover, the examiner does not allege, and Applicant cannot find the teaching of "providing service provider identifiers to each person that identifies the respective persons to a service provider" in Kesarwani or Nordman either. Accordingly, at least this feature is not taught in the cited references.

The examiner now also alleges that Kesarwani teaches the claimed message transmitting step and authorizing step at column 6, lines 29-38. However, the cited passage of Kesarwani merely teaches comparing login, password and security information to access rules to allow access to information stored in a main office. Applicant still can find no teachings in Kesarwani related to the claimed steps of:

> transmitting a message from one of the persons to the service provider through the pseudonymous proxy server, wherein the pseudonymous proxy server receives the message and, based on the set of rules that control said one person's access to the stored private data of a person registered with the pseudonymous proxy server, validates a relationship between said one person and the service provider and transmits the message to the service provider if the relationship between said one person and the service provider is validated; and
>
> said pseudonymous proxy server authorizing said one person to view the stored private data of said person or pseudonyms for said private data of said person based on said set of rules that control said one person's access to

said stored private data of said person and said pseudonyms for said private data of said person.

Kesarwani teach the use of access rules to control a user's access to stored information using access rules including, for example, "security access codes, passwords, login IDs, and access information" (column 4, lines 61-63). Kesarwani's access rules apply to accessing the database *generally* – not the private data or pseudonyms for the private data for a particular individual stored in the database. Thus, Kesarwani. do not validate a relationship between the person and the service provider *for allowing the person to view stored private data or pseudonyms of the private data* as claimed in claim 1 or between the person and the owner of the stored private data as now claimed in new claim 6 and then transmit the message if the relationship is validated. Accordingly, this feature also is not taught in the cited references.

Finally, the examiner again alleges based on the teachings of Nordman at paragraphs [0013] and [0094] that applying a random factor to the generated pseudonym "is a logical extension of Smirnov, Ho, and Kesarwani." However, while Nordman suggests substituting "randomized pseudonym addresses for the device's real unique address, to confer anonymity upon the user," Nordman does not teach applying a random factor to the person's pseudonym or the service provider identifier as claimed.

Applicant again submits that, for at least the reasons indicated, the teachings of Smirnov, Ho, Kesarwani and Nordman would not have been combined by one skilled in the art to arrive at the method of claim 1. On the contrary, as has been noted above, the cited prior art provides access to data based on the relationships of the system users to the system elements as opposed to based on relationships of the stored data to those desiring access and to do so without disclosing the identify of the owner of the data. Such features are not taught in any of the cited references. Combining the teachings of the references does not overcome such omissions. Thus, even if the teachings of Smirnov, Ho, Kesarwani, and Nordman could somehow have been combined by one skilled in the art as the examiner alleged, the claimed invention would not have resulted. Withdrawal of the rejection of claim 1 is appropriate and is solicited.

Dependent claims 2-6 are believed to be allowable by virtue of their dependence upon allowable claim 1. Moreover, claim 5 further distinguishes over the cited references by reciting "pseudonymizing the person's medical records in accordance with the another medical service provider's access rights, and providing the access rights to the another medical service provider based on authorization to the person's medical records as granted by the person." No such teachings are provided by Smirnov, Ho, Kesarwani, or Nordman taken alone or together. Claim 6 is also believed to further distinguish over the cited references by reciting validating a relationship between the person requesting access to the stored private data and the owner of the stored private data and transmitting the message to the service provider if the relationship between the person and the owner of the stored private data is validated. Absent such teachings, claims 5 and 6 are believed to clearly distinguish over the cited prior art.

Allowance of dependent claims 2-6 is thus appropriate and is further requested.

Conclusion

In view of the above amendments and remarks, claims 1-6 are believed to be in condition for allowance. A Notice of Allowability is respectfully solicited.

Date: December 8, 2009

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439